AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for facilitating secure communication between two networked devices, comprising:

establishing communication between a situation notification device and a provisioning device over a preferred channel, wherein the preferred channel is bidirectional, location-limited, has a demonstrative identification property and an authenticity property, and does not require being resistant to eavesdropping;

> wherein the demonstrative identification property allows a human operator to be aware of which devices are communicating with each other based on physical proximity; and
>
> wherein the authenticity property makes it difficult or impossible for attacking devices to tamper with or alter messages transmitted in the preferred channel, or to insert false information into the preferred channel without being detected by legitimate participants communicating via the preferred channel;

prior to establishing the communication, pre-authenticating the situation notification device to ensure that the situation notification device has physical access to the preferred channel, wherein pre-authenticating the situation notification device involves:

> exchanging key commitment information between the provisioning device and the situation notification device over the bidirectional preferred channel;

exchanging keys between the provisioning device and the situation notification device over a bidirectional channel which does not have to be the preferred channel; and

verifying the received keys using the received key commitment information on both the provisioning device and the situation notification device;

providing provisioning information to said situation notification device over said preferred channel, wherein said situation notification device is automatically configured to receive subject matter information responsive to said provisioning information;

receiving said subject matter information;

verifying said subject matter information with said provisioning information; and

presenting said subject matter information to a user of the situation notification device responsive to the step of verifying, wherein the step of verifying ensures that the subject matter information is genuine.

2. (Previously presented) The method of claim 1, wherein the step of providing further comprises:

exchanging key commitment information over said preferred channel between said provisioning device and said situation notification device;

receiving a public key by said situation notification device;

verifying said public key with said key commitment information; and

receiving a credential authorized by a credential issuing authority.

3. (Previously presented) The method of claim 1, wherein said preferred channel is a location-limited channel.

4. (Previously presented) The method of claim 1, wherein said preferred channel uses a telephone switching system.

5. (Canceled)

6. (Previously presented) The method of claim 1, wherein subject matter information is received using an antenna, a telephone line, a local area network, a wide area network, a wireless network, or a broadcast network.

7. (Previously presented) The method of claim 1, wherein said situation notification device is a computer, a television, a radio, a telephone, a push to talk device, a pager, a clock, a thermostat, a network appliance, or a home appliance.

8. (Previously presented) The method of claim 1, further comprising forwarding said subject matter information.

9. (Previously presented) The method of claim 1, wherein said subject matter information is alarm information.

10. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to present subject matter information, the method comprising steps of:

establishing communication between a situation notification device and a provisioning device over a preferred channel, wherein the preferred channel is bidirectional, location-limited, has a demonstrative identification property and an authenticity property, and does not require being resistant to eavesdropping;

wherein the demonstrative identification property allows a human operator to be aware of which devices are communicating with each other based on physical proximity; and

wherein the authenticity property makes it difficult or impossible for attacking devices to tamper with or alter messages transmitted in the preferred channel, or to insert false information into the preferred channel without being detected by legitimate participants communicating via the preferred channel;

prior to establishing the communication, pre-authenticating the situation notification device to ensure that the situation notification device has physical access to the preferred channel, wherein pre-authenticating the situation notification device involves:

exchanging key commitment information between the provisioning device and the situation notification device over the bidirectional preferred channel;

exchanging keys between the provisioning device and the situation notification device over a bidirectional channel which does not have to be the preferred channel; and

verifying the received keys using the received key commitment information on both the provisioning device and the situation notification device;

providing provisioning information to said situation notification device over said preferred channel, wherein said situation notification device is automatically configured to receive said subject matter information responsive to said provisioning information;

receiving said subject matter information;

verifying said subject matter information with said provisioning information; and presenting said subject matter information to a user of the situation notification device responsive to the step of verifying, wherein the step of verifying ensures that the subject matter information is genuine.

11. (Original) The computer-readable storage medium of claim 10, wherein the step of providing
further comprises:

exchanging key commitment information over said preferred channel between said provisioning device and said situation notification device;

receiving a public key by said situation notification device;

verifying said public key with said key commitment information; and

receiving a credential authorized by a credential issuing authority.

12. (Original) The computer-readable storage medium of claim 10, wherein said preferred channel is a location-limited channel.

13. (Original) The computer-readable storage medium of claim 10, wherein said preferred channel uses a telephone switching system.

14. (Canceled)

15. (Original) The computer-readable storage medium of claim 10, wherein subject matter information is received using an antenna, a telephone line, a local area network, a wide area network, a wireless network, or a broadcast network.

16. (Original) The computer-readable storage medium of claim 10, wherein said situation notification device is a computer, a television, a radio, a

telephone, a push to talk device, a pager, a clock, a thermostat, a network appliance, or a home appliance.

17. (Original) The computer-readable storage medium of claim 10, further comprising forwarding said subject matter information.

18. (Original) The computer-readable storage medium of claim 10, wherein said subject matter information is alarm information.

19. (Currently amended) An apparatus comprising:

at least one port configured to establish a preferred channel, wherein the preferred channel is bidirectional, location-limited, has a demonstrative identification property and an authenticity property, and does not require being resistant to eavesdropping;

> wherein the demonstrative identification property allows a human operator to be aware of which devices are communicating with each other based on physical proximity; and
>
> wherein the authenticity property makes it difficult or impossible for attacking devices to tamper with or alter messages transmitted in the preferred channel, or to insert false information into the preferred channel without being detected by legitimate participants communicating via the preferred channel;

a first communication mechanism configured to receive provisioning information over said preferred channel, whereby the apparatus is configured to be able to receive subject matter information responsive to said provisioning information,

wherein the port is further configured to pre-authenticate the first communication mechanism prior to receiving the provisioning information to ensure that the first communication mechanism has physical access to the preferred channel, wherein pre-authenticating the situation notification device involves:

exchanging key commitment information between the provisioning device and the situation notification device over the bidirectional preferred channel;

exchanging keys between the provisioning device and the situation notification device over a bidirectional channel which does not have to be the preferred channel; and

verifying the received keys using the received key commitment information on both the provisioning device and the situation notification device;

a second communication mechanism configured to receive said subject matter information subsequent to operation of the first communication mechanism;

a verification mechanism configured to verify said subject matter information with said provisioning information; and

a presentation mechanism configured to present said subject matter information to a user of the situation notification device responsive to the verification mechanism, wherein the step of verifying ensures that the subject matter information is genuine.

20. (Original) The apparatus of claim 19, wherein the first communication mechanism further comprises:

a key commitment receiver mechanism configured to receive key commitment information through said at least

one port;

a key receiver mechanism configured to receive a public key;

a pre-authentication mechanism configured to verify said public key with said key commitment information; and

a credential provisioning mechanism configured to be able to automatically provide a credential authorized by a credential issuing authority responsive to the pre-authentication mechanism.

21. (Original) The apparatus of claim 19, wherein said preferred channel is a location-limited channel.

22. (Original) The apparatus of claim 19, wherein said preferred channel uses a telephone switching system.

23. (Canceled)

24. (Original) The apparatus of claim 19, wherein subject matter information is received using an antenna, a telephone line, a local area network, a wide area network, a wireless network, or a broadcast network.

25. (Original) The apparatus of claim 19, wherein the apparatus is within a computer, a television, a radio, a telephone, a push to talk device, a pager, a clock, a thermostat, a network appliance, or a home appliance.

26. (Original) The apparatus of claim 19, further comprising a forwarding mechanism configured to forward said subject matter information.

27. (Original) The apparatus of claim 19, wherein said subject matter information is alarm information.

28. (Previously Presented) The method of claim 1, wherein said preferred channel has a demonstrative identification property and an authenticity property

29. (Previously Presented) The computer-readable storage medium of claim 10, wherein said preferred channel has a demonstrative identification property and an authenticity property.

30. (Previously Presented) The apparatus of claim 19, wherein said preferred channel has a demonstrative identification property and an authenticity property.